Secrecy Communication with Security Rate Measure

Lei Yu, Houqiang Li, and Weiping Li, *Fellow, IEEE*
University of Science and Technology of China
Email: yulei@mail.ustc.edu.cn, {lihq,wpli}@ustc.edu.cn

***Abstract*—We introduce a new measure on secrecy, which is established based on rate-distortion theory. It is named *security rate*, which is the minimum (infimum) of the additional rate needed to reconstruct the source within target distortion level with any positive probability for wiretapper. It denotes the minimum distance in information metric (bits) from what wiretapper has received to any decrypted reconstruction (where decryption is defined as reconstruction within target distortion level with some positive possibility). By source coding theorem, it is equivalent to a distortion-based equivocation $\min_{p(v^n|s^n,m):Ed(S^n,V^n)\leq D_E} \frac{1}{n} I(S^n;V^n|M)$ which can be seen as a direct extension of equivocation $\frac{1}{n}H(S^n|M)$ to lossy decryption case, given distortion level D_E and the received (encrypted) message M of wiretapper. In this paper, we study it in Shannon cipher system with lossless communication, where a source is transmitted from sender to legitimate receiver secretly and losslessly, and also eavesdropped by a wiretapper. We characterize the admissible region of secret key rate, coding rate of the source, wiretapper distortion, and security rate (distortion-based equivocation). Since the security rate equals the distortion-based equivocation, and the equivocation is a special case of the distortion-based equivocation (with Hamming distortion measure and $D_E = 0$), this gives an answer for the meaning of the maximum equivocation.**

I. Introduction

The Shannon cipher system depicted in Fig. 1 is first investigated in [1], where sender A communicates with legitimate receiver B secretly by exploiting a secret key that is shared by them. In [1], Shannon regarded this system as perfectly secret if the source and the eavesdropped message are statistically independent. For lossless communication case, a necessary and sufficient condition for perfect secrecy is that the number of secret key bits per source symbol exceeds the entropy of the source. When the amount of key is insufficient, it must relax the requirement of statistical independence and introduce new measures of secrecy.

One common way of measuring sub-perfect secrecy is with equivocation, the conditional entropy $\frac{1}{n}H(S^n|M)$ of the source given the public message. The use of equivocation as a measure of secrecy was considered in the original work on the wiretap channel in [2] and [3], and it continues today. From lossy source coding theorem, the equivocation indeed indicates the minimum additional rate for wiretapper to reconstruct the source losslessly on the basis of the received message M, when the coding scheme adopted by A and B is stationary.

For lossy decryption, a distortion-based measure has been proposed by Yamamoto in [4], which is to measure secrecy by the distortion that an wiretapper incurs in attempting to reconstruct the source sequence. However, Schieler et al [5] show that this measure is cheap, since negligible rates of secret key can force minimum distortion achieved by wiretapper to the one reconstructed without any information about the source; meanwhile it is also fragile, since wiretapper can reconstruct the transmitted message completely if it has a little knowledge of the source. To strengthen measure of secrecy, another distortion-based approach [6], [7] is to design schemes around the assumption that the wiretapper has ability to conduct list decoding with fixed list size. The induced distortion is the minimum distortion over the entire list. This exponent of list size R_L is an important indicator to secrecy performance. From aspect of uncertainty, R_L indeed indicates the minimum additional rate needed to reconstruct the source within target distortion level with "zero-delay" decryption constraint, where "zero-delay" follows from that only single-block codes are allowed for wiretapper, i.e., the blocklength adopted by wiretapper is restricted to be the same to that adopted by A and B (in fact, without delay constraint, the wiretapper would collect multiple blocks to produce a supperblock reconstruction, which is called *superblock coding*). This quantity is somewhat similar to equivocation (i.e., $\frac{1}{n}H(S^n|M)$), which is also to measure the uncertainty of the wiretapper. However the equivocation is the minimum additional rate to decrypt for henchman and wiretapper, when wiretapper could apply arbitrary length supercode; while for R_L, only single-block codes are allowed for wiretapper. In addition, from aspect of complexity, R_L indicates the exponent of admissible maximum complexity (exponent of admissible maximum list size over all blocks) needed to reconstruct the source within target distortion level.

In this paper, we study the Henchman problem with superblock coding, and define security rate as the minimum (infimum) of the additional rate needed to reconstruct the source within target distortion level with any positive probability for wiretapper. We aim at characterizing the optimal tradeoff among secret key rate, coding rate of the source, wiretapper distortion D_E, and security rate. An important difference from [6] is that we do not constrain the blocklength adopted by the Henchman and wiretapper; while in [6], the blocklength adopted by the Henchman and wiretapper is restricted to be the same to that adopted by A and B. It is worth noting that the proof in [6] relies on a likelihood encoder by using the soft covering lemma [8], which is invalid to solve our problem.

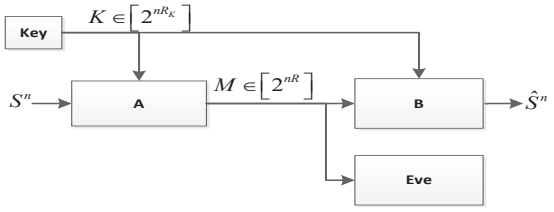

Figure 1: The Shannon cipher system.

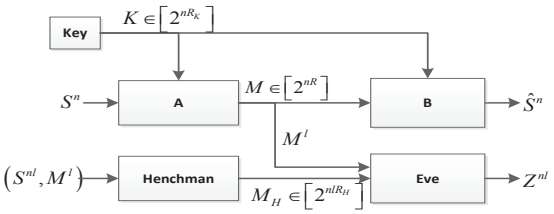

Figure 2: The henchman problem with superblock coding. A henchman who has access to the l blocks of source sequence, S^{nl}, and the l blocks of public message, M^l, codes them with rate R_H to help wiretapper to produce a reconstruction. The wiretapper reconstructs a sequence Z^{nl} based on the public message M^l and the information M_H from the henchman. Here $M^l = (M_1, M_2, \cdots, M_l)$ denotes a sequence of the messages M.

This is because if consider the superblock case and let $l \to \infty$ before let $n \to \infty$, then the soft covering lemma does not hold, where l denotes the number of subblocks in each supperblock, and n denotes the number of symbols in each subblock (which is also the blocklength of the code adopted by A and B). Actually, we find a more general approach to solve our problem which relies on jointly typical coding. Moreover, our approach is available to prove the results of [6]. In addition, we also define distortion-based equivocation as $\min_{p(v^n|s^n,m):Ed(S^n,V^n)\le D_E} \frac{1}{n} I\left(S^n; V^n|M\right)$, which can be seen as an extension of equivocation $\frac{1}{n} H\left(S^n|M\right)$ to lossy decryption case. By source coding theorem, in our problem the security rate is exactly equal to the distortion-based equivocation. Hence utilizing the result on security rate, we can easily characterize the admissible region of secret key rate, coding rate of the source, wiretapper distortion D_E and distortion-based equivocation by replacing security rate with distortion-based equivocation. It means that maximizing equivocation is indeed equivalent to maximizing security rate of lossless decryption. We also extend our results on lossless communication case to lossy communication case.

II. Problem Formulation and Preliminaries

Consider the secrecy communication system shown in Fig. 1. The sender A observes a source sequence S^n that is i.i.d. according to a distribution P_S . Sender A and legitimate receiver B share a secret key K that is uniformly distributed in $\left[2^{nR_K}\right]$ [1] and independent of S^n. Sender A encodes the source using the secret key and then sends the coded message M to legitimate receiver B over a noiseless channel at rate R, which is also wiretapped by a wiretapper Eve. To make our problem more clear, we introduce the Henchman problem with supperblock coding shown in Fig. 2 (the single block coding version is investigated in [6]).

Henchman problem with supperblock coding

Definition 1. *The encoder and decoder of a (n, R, R_K) block code are defined by the following two mappings:*

$$\begin{aligned} &Encoder\ f : \mathcal{S}^n \times \left[2^{nR_K}\right] \to \left[2^{nR}\right] \\ &Decoder\ g : \left[2^{nR}\right] \times \left[2^{nR_K}\right] \to \hat{\mathcal{S}}^n \end{aligned} \tag{1}$$

The wiretapper Eve overhears the encrypted message M perfectly. A and B want to communicate within certain distortion level by using the secret key and the noiseless channel, while ensuring that the wiretapper suffers distortion above a certain threshold with high probability. We say a source sequence s^n is decrypted by wiretapper if and only if the wiretapper produces a reconstruction of s^n, z^n, such that

$$d\left(s^n, z^n\right) \le D_E \tag{2}$$

When D_E is small enough, and A and B adopt an appropriate coding scheme, then the wiretapper cannot decrypt the source only by M. Hence, we can measure security by the minimum additional bit rate needed for wiretapper to decrypt the source. In this case, it is equivalent to that there is a rate-limited helper (i.e., a henchman) who can access all information about source (source S^n and the encrypted message M). As depicted in Fig. 2, by applying an l- length of superblock code (each subblock with n symbols), the wiretapper receives nlR_H bits of side information from a henchman who has access to the source sequence S^{nl} and the public message M^l. Since the wiretapper and henchman cooperate, this means that the wiretapper effectively receives the best possible nlR_H bits of side information about the pair $\left(S^{nl}, M^l\right)$ to assist in producing a reconstruction sequence Z^{nl}.

Definition 2. *The (l, R_H) Henchman code (Hcode) of a (n, R, R_K) block code is a superblock defined by the following two mappings:*

$$\begin{aligned} &Encoder\ f_H : \mathcal{S}^{nl} \times \left[2^{nlR}\right] \to \left[2^{nlR_H}\right] \\ &Decoder\ g_H : \left[2^{nlR_H}\right] \times \left[2^{nlR}\right] \to \mathcal{Z}^{nl} \end{aligned} \tag{3}$$

The encoder and decoder of Hcode can be stochastic.

For any (n, R, R_K) block code, we define security rate to measure its secrecy.

Definition 3. *For an (n, R, R_K) block code adopted by A and B, and a given decryption distortion level D_E, Henchman rate R_H of the (n, R, R_K) block code is said to be secure if for $\forall \epsilon > 0$, the following inequality holds. In this case, R_H is said to be a secure Henchman rate or security rate.*

$$\limsup_{l\to\infty} \max_{\substack{(l, R'_H)\, Hcodes \\ R'_H \le R_H - \epsilon}} \mathbb{P}\left[d\left(S^{nl}, Z^{nl}\right) \le D_E\right] \le \epsilon \tag{4}$$

[1] In this paper, the set $1, \ldots, m$ is sometimes denoted by $[m]$.

From Definition 3, we have that if the wiretapper receives any additional message with rate $\leq$ security rate, then it cannot reconstruct the source within target distortion level with probability$\geq \epsilon$ for any $\epsilon > 0$. Security rate also denotes the infimum of the additional rate needed to reconstruct the source within target distortion level with probability$\geq \epsilon$ for any $\epsilon > 0$ for wiretapper.

To keep the transmission as secret as possible from Eve, A and B should maximize security rate or minimize decryption probability in (4).

Definition 4. *The tuple (R, R_K, R_H, D_E) is achievable for distortion measure d if for $\forall \epsilon > 0$, as well as sufficiently large n, there exists an (n, R', R'_K) code satisfying*

$$R'_K \leq R_K + \epsilon \tag{5}$$
$$R' \leq R + \epsilon \tag{6}$$
$$\mathbb{P}\left[S^n \neq \hat{S}^n\right] \leq \epsilon \tag{7}$$
$$R_H(D_E) \geq R_H - \epsilon \tag{8}$$

Inequality (8) is equivalent to (4).

Definition 5. *Given R, R_K, and D_E, maximum security rate $R^*_H(R, R_K, D_E)$ is defined as the supremum of all R_H such that (R, R_K, R_H, D_E) is achievable.*

The wiretapper and henchman jointly design a code consisting of an encoder $m_H = f_H\left(s^{nl}, m^l\right)$ and a decoder $z^{nl} = g_H\left(m_H, m^l\right)$, subject to the constraint $|M_H| \leq 2^{nlR_H}$. We assume that the henchman and the wiretapper are both aware of the scheme that Nodes A and B employ, but neither aware of the secret key. That is to say the $f_H\left(s^{nl}, m^l\right), g_H\left(m_H, m^l\right)$ may be designed based on the (n, R, R_K) block code.

Although we assume the excess distortion constraint constraint of distortion for wiretapper here, from the proofs of our results, our results still hold if apply expected distortion constraint for wiretapper [2].

In addition, it is worth noting that based on the definitions above, maximum security rate is equivalent to the following definition.

Definition 6. *For a (n, R, R_K) block code adopted by A and B, and for a given decryption distortion level D_E, distortion-based equivocation is defined as:*

$$R_{DE}(D_E) = \min_{\substack{p(v^n|s^n,m):\\ Ed(S^n,V^n) \leq D_E}} \frac{1}{n} I\left(S^n; V^n | M\right) \tag{9}$$

The distortion-based equivocation is exactly a direct extension of equivocation to lossy decryption case. For maximum security rate in Definition 5 we restrict the code adopted by A and B to be stationary (independent of time), hence the outputs M^l must be a stationary process. Then by source coding theorem, $R_{DE}(D_E)$ is the minimum additional rate to decrypt source with any positive probability for henchman and wiretapper. Therefore, maximum $R_{DE}(D_E)$ is exactly equal to $R^*_H(R, R_K, D_E)$. This implies that maximum equivocation is equal to the maximum security rate of lossless decryption.

[2]Assume the distortion function is upper bounded.

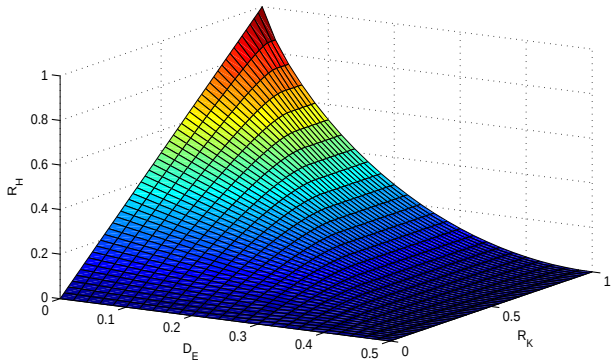

Figure 3: The region in Theorem 1 for source $P_S \sim$Bern(1/2) and distortion measure $d(s,z) = 1\{s \neq z\}$.

III. Main Results

The following theorem characterizes the admissible region for lossless communication among the communication rate, secret key rate, wiretapper distortion, and security rate.

Theorem 1. *Given a source distribution P_S and distortion measure d, the tuple (R, R_K, R_H, D_E) is achievable if and only if it holds that*

$$R \geq H(S), \tag{10}$$
$$R_H \leq \Gamma(R_K, D_E) \tag{11}$$

where

$$\Gamma(R_K, D_E) \triangleq \min_{\substack{(\lambda, D): 0 \leq \lambda \leq 1,\\ \lambda D \leq D_E}} (1-\lambda) R_K + \lambda R(D) \tag{12}$$

$R(D)$ denotes rate-distortion function of source S with distortion measure $d(s, \hat{s})$, i.e.,

$$R(D) = \min_{p(v|s): Ed(S,V) \leq D} I(S; V) \tag{13}$$

The function (12) is exactly the rate-distortion tradeoff of the timesharing between the points $(0, R_K)$ and $(D, R(D))$. Note that the region of Theorem 1 is different from that in Theorem 1 of [6], which is the singleblock coding version of Henchman problem. More precisely, the region of Theorem 1 is the convex hull of that in Theorem 1 of [6] in R_H and D_E dimensions. This is because the timesharing is feasible for superblock coding, but not feasible for singleblock coding. It also implies that timesharing is one of the optimal strategies to achieve the optimal R_H and D_E tradeoff. Fig. 3 illustrates Theorem 1 for a Bern(1/2) source and Hamming distortion; the communication rate is assumed to satisfy $R \geq H(S)$, and they have no effect on the (R_K, R_H, D_E) tradeoff. In Fig. 3,

for given R_K and R_H, the distortion region below the surface is not achievable for wiretapper with probability 1; while the distortion region above the surface is achievable for wiretapper with probability 1.

We can readily establish the following corollaries to Theorem 1.

Corollary 1. *Given a source distribution P_S and distortion measure d, for all $R \geq H(S)$,*

$$R_H^*(R, R_K, D_E) = \Gamma(R_K, D_E) \tag{14}$$

From the fact maximum $R_{DE}(D_E)$ is equal to $R_H^*(R, R_K, D_E)$, we have the following corollary.

Corollary 2. *Given $R \geq H(S)$ and R_K, maximum $R_{DE}(D_E)$ equals the $R_H^*(R, R_K, D_E)$, i.e., they satisfy*

$$\begin{aligned} &\limsup_{n\to\infty} \max_{\substack{(n, R', R'_K)\, codes \\ R' \leq R, R'_K \leq R_K}} R_{DE}(D_E) \\ =&R_H^*(R, R_K, D_E) \qquad (15) \\ =&\Gamma(R_K, D_E) \qquad (16) \end{aligned}$$

In addition, for lossless reconstruction at wiretapper, observe that $\limsup_{n\to\infty} \max_{\substack{(n, R', R'_K)\, codes \\ R' \leq R, R'_K \leq R_K}} \frac{1}{n} H(S^n|M)$ equals $\limsup_{n\to\infty} \max_{\substack{(n, R', R'_K)\, codes \\ R' \leq R, R'_K \leq R_K}} R_{DE}(0)$ with Hamming distortion measure, hence by Corollary 2 the maximum equivocation is indeed equal to the maximum security rate.

Corollary 3. *Given $R \geq H(S)$ and R_K, maximum equivocation equals the $R_H^*(R, R_K, D_E = 0)$, with Hamming distortion measure and also equals $\Gamma(R_K, D_E = 0)$.*

Note that when setting $d(s, \hat{s}) = 1\{s \neq \hat{s}\}$ in the region of Corollary 3, corresponds to requiring a lossless reconstruction at wiretapper, which was Shannon's original formulation of the problem in [1]. In this case, we see that the tuple $(R, R_K, R_H, D_E = 0)$ is achievable if and only if

$$R \geq H(S) \tag{17}$$

$$\limsup_{n\to\infty} \max_{\substack{(n, R', R'_K)\, codes \\ R' \leq R, R'_K \leq R_K}} R_{DE}(0) = \min\{R_K, H(S)\} \tag{18}$$

This implies the Shannon's results [1], i.e., the perfect secrecy (equivocation equals $H(S)$) is achievable if and only if $R_K \geq H(S)$.

We now prove the achievability and converse parts of Theorems 1.

IV. Converse of Theorem 1

The constraint $R \geq H(S)$ follows from the lossless source coding theorem. If $R_H \geq R_K$, then the henchman can send the index of possible decryptions of M. For any scheme that Nodes A and B use, Node B can always use the rate-R_K key to identify the correct decryption of M (with probability 1), hence the number of possible decryptions of M is at most 2^{nR_K}. This means that it is possible for the wiretapper to produce a lossless reconstruction (with probability 1) with henchman rate R_H. On the other hand, if $R_H \geq R(D_E)$, then the henchman and the wiretapper can simply use a point-to-point rate-distortion code (ignore M altogether) to describe S^n within distortion D_E (with probability 1), no matter what scheme Nodes A and B use. In addition, by applying time-sharing, the the henchman and the wiretapper are able to achieve any distortion-rate pair on or above the convex hull of $(D, \min\{R_K, R(D)\})$. Hence, to prevent wiretapper from achieving that, the inequality(11) holds.

V. Achievability of Theorem 1

To prove the achievability, we only need to prove that if (10) and (11) hold, then there exists a code (adopted by A and B) making (4) hold. It means that the henchman observes the pair $\left(S^{nl}, M^l\right)$ and encodes a message M_H, and the wiretapper observes $\left(M^l, M_H\right)$ and decodes Z^{nl}; their goal is to minimize the distortion $d\left(S^{nl}, Z^{nl}\right)$. This is just the usual rate-distortion setting with side information M^l available at both encoder and decoder. We will prove that if the Node A and B use the following coding scheme to encode and decode the source sequence, then (4) holds.

Generation of codebooks: First, randomly generate a codebook $\mathcal{C}_S$ consisting of 2^{nR} sequences S^n drawn i.i.d. $\sim \prod_{i=1}^n P_S(s_i)$. Then divide all the codewords into bins of size 2^{nR_K}. Index bins by $j_p \in \left[2^{n(R-R_K)}\right]$ and denote them as $\mathcal{C}_S(j_p)$. Also index codewords of each bin by $j_s \in \left[2^{nR_K}\right]$. The codebook as well as binning and indexing are known to everyone, including the adversaries (henchman and wiretapper).

Encoding at sender: Sender encode the sequence s^n by $j = (j_p, j_s)$ if there exists an (j_p, j_s) pair such that $s^n = s^n(j_p, j_s)$ in codebook $\mathcal{C}_S$ and $s^n(j_p, j_s) \in \mathcal{T}_\delta^n$ (This is equivalent to find an (j_p, j_s) pair such that $(s^n, s^n(j_p, j_s)) \in \mathcal{T}_\delta^n\left(S, \hat{S}\right)$, where test channel $P_{\hat{S}|S}(\hat{s}|s) = 1\{\hat{s} = s\}$). If there is more than one such index, randomly (uniformly) choose one among them. If there is no such index, randomly choose one index from $\left[2^{nR}\right]$. Then the index within that bin, j_s, is one-time padded with the key sequence k. Denote the message to $m = (j_p, m_s)$, where m_s denotes the resulting message by one-time pad operation on j_s with k.

Decoding at legitimate receiver: Using the key k, legitimate receiver achieves (j_p, j_s) from the received m, and then it reproduces the sequence $s^n(j_p, j_s)$.

By the standard proof on lossless source coding using joint typicality coding, we can readily establish that if $R > H(S)$, then the legitimate receiver can reconstruct S^n with high probability. Hence, we only need to prove that based on received M, with high probability it is impossible for wiretapper to achieve distortion less than D_E, if R_H satisfies (11).

Theorem 2. *Let τ_n be any sequence that converges to zero sub-exponentially fast (i.e., $\tau_n = 2^{-o(n)}$). If*

$$R_H \leq \Gamma\left(R_K, D_E\right) \tag{19}$$

then for $\forall \epsilon > 0$,

$$\lim_{n\to\infty} \mathbb{P}_{\mathcal{C}_S}\Big[\limsup_{l\to\infty} \mathbb{E}_{M^l} \max_{\substack{(l, R'_H)\, H codes: \\ R'_H \leq R_H - \epsilon}} \mathbb{P}\left[d\left(S^{nl}, Z^{nl}\right) \leq D_E\right] > \tau_n\Big] = 0 \tag{20}$$

where $\Gamma(\cdot)$ is defined in (12), and $M^l = (M_1, M_2, \cdots, M_l)$.

The proof is given in Appendix B.

Then by Theorem 2 we can establish the following corollary.

Corollary 4. *If R_H satisfies (11), then for $\forall \epsilon > 0$,*

$$\lim_{n\to\infty} \mathbb{E}_{\mathcal{C}_S}\Big[\limsup_{l\to\infty} \mathbb{E}_{M^l} \max_{\substack{(l, R'_H)\, H codes: \\ R'_H \leq R_H - \epsilon}} \mathbb{P}\left[d\left(S^{nl}, Z^{nl}\right) \leq D_E\right]\Big] = 0 \tag{21}$$

The Corollary 4 implies (11) of Theorem 1. Hence the proof is completed.

VI. Causal Encryption System

Here we consider a more general secrecy system, "causal encryption system". Consider the secrecy communication system in Fig. 1, where the key is delivered at rate R_K, and the sender can not only use the current key but also all past keys to code the current block. We assume that the wiretapper has no decryption-delay constraint, hence it can do decryption after receving all transmitted blocks (assume total number is L). Besides, since the sender could adopt such an adaptive encryption scheme (amount of key could be different for different blocks), we assume the henchman and the wiretapper could also arrange any l transmitted blocks to form a superblock.

Let the sender only use the current key, then this kind of general secrecy system is degenerated into the system described in Section II. By using the same compression and encryption scheme in Section V, the sender and the receiver could achieve the same secrecy performance. Hence for causal encryption system, the achievablity of Theorem 1 still holds. In addition, for the first $(1-\lambda)L$ blocks, the henchman can use rate-R_K henchman code to help the wiretapper produce a lossless reconstruction (with probability 1), and for the last λL blocks, the henchman can use rate-$R(D_E)$ henchman code to help the wiretapper produce a reconstruction of S^n within distortion D_E (with probability 1). Hence, the average henchman rate is $(1-\lambda)R_K + \lambda R(D_E)$, and the average distortion is λD_E. This means that the converse part of Theorem 1 still holds as well. Hence the achievable (R, R_K, R_H, D_E) for this case is also given by Theorem 1.

VII. Conclusion

In this paper, we introduce a new measure on secrecy, *security rate*, which is established based on rate-distortion theory, and denotes the minimum (infimum) of the additional rate needed to reconstruct the source within target distortion level with any positive probability for wiretapper. We study it in Shannon cipher system with lossless communication, and characterize the admissible region of secret key rate, coding rate of the source, wiretapper distortion, and security rate (distortion-based equivocation). The single block version of henchman problem has been studied in [6] and [7]. In addition, by applying time-sharing decryption strategy, in the superblock version, the henchman and the wiretapper are able to achieve any distortion-rate pair on or above the convex hull of (D, R_H) of the single block version. Moreover, we prove that such time-sharing decryption strategy is optimal. In addition, since the security rate equals the distortion-based equivocation, $\min_{p(v^n|s^n,m):Ed(S^n,V^n)\leq D_E} \frac{1}{n} I\left(S^n; V^n|M\right)$, and the equivocation is a special case of the distortion-based equivocation (with Hamming distortion measure and $D_E = 0$), this gives an answer for the meaning of the maximum equivocation.

References

[1] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1334–1387, 1975.

[3] I. Csiszár, and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 827–835, May 1997.

[5] C. Schieler and P. Cuff, "Rate-distortion theory for secrecy systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7584–7605, Nov. 2014.

[6] C. Schieler, and P. Cuff, "The henchman problem: measuring secrecy by the minimum distortion in a list," in *Proc. IEEE International Symposium on Information Theory*, Honolulu, HI, pp. 596–600, Jun. 2014.

[7] C. Schieler, and P. Cuff, "The henchman problem: measuring secrecy by the minimum distortion in a list," submitted to *IEEE Trans. on Inf. Theory*, October, 2014.

[8] P. Cuff, "Distributed channel synthesis," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7071–7096, 2013.

[9] H. Palaiyanur and A. Sahai, "On the uniform continuity of the rate-distortion function," in *Proc. IEEE Int. Symp. on Information Theory (ISIT)*, Jul. 2008, pp. 857–861.

[10] I. Csiszár, and J. Körner, Information Theory: Coding Theorems for Discrete Memoryless Systems. New York: Academic, 1981.

[11] A. El Gamal and Y.-H. Kim, Network Information Theory. Cambridge University Press, 2011.

[12] M. Mitzenmacher and E. Upfal, Probability and Computing: Randomized Algorithms and Probabilistic Analysis. Cambridge University Press, 2005.

APPENDIX A
PROPERTY OF DISTORTION SET

Proposition 1. *(Property of Distortion Set): For any distortion measure $d(s^n, z^n)$, if both $|\mathcal{S}|$ and $|\mathcal{Z}|$ are finite, then the cardinality of $\mathcal{D}^n \triangleq \{d(s^n, z^n) : s^n \in \mathcal{S}^n, z^n \in \mathcal{Z}^n\}$ is at most polynomial in n.*

Proof: Observe that the term $d(s^n, z^n)$ only depends on the joint type of (s^n, z^n), and moreover the number of joint types is at most $(n+1)^{|\mathcal{S}||\mathcal{Z}|}$ [10], which is polynomial in n. ■

APPENDIX B
PROOF OF THEOREM 2

Proof: We first define four envents

$$\mathcal{A}_1 \triangleq \{S^n \in \mathcal{T}_\delta^n, S^n \in \mathcal{C}_S\}, \tag{22}$$

$$\mathcal{A}_2 \triangleq \left\{ \begin{array}{l} \max\limits_{j_p \in \left[2^{n(R-R_K)}\right]} \max\limits_{z^n \in \mathcal{Z}^n} \eta_{\mathcal{C}_S, D}(z^n, j_p) \\ \leq 2^{n\left([R_K - R(D)]^+ + \epsilon\right)}, \forall D \in \mathcal{D}^n \end{array} \right\}, \tag{23}$$

$$\mathcal{A}_3 \triangleq \left\{ \min_{j_p \in \left[2^{n(R-R_K)}\right]} \gamma_{\mathcal{C}_S}(j_p) \geq (1-\epsilon) 2^{nR_K} \right\}, \tag{24}$$

$$\mathcal{A}_4 \triangleq \left\{ \begin{array}{l} \max\limits_{s^n \in \mathcal{T}_\delta^n} \phi_{\mathcal{C}_S}(s^n) \leq 2^{n(R-H(S)+\epsilon)}, \\ \min\limits_{s^n \in \mathcal{T}_\delta^n} \phi_{\mathcal{C}_S}(s^n) \geq 2^{n(R-H(S)-\epsilon)} \end{array} \right\}, \tag{25}$$

where

$$\eta_{\mathcal{C}_S, D}(z^n, j_p) \triangleq \sum_{j_s=1}^{2^{nR_K}} 1\left\{ d\left(S^n(j_p, j_s), z^n\right) \leq D, S^n(j_p, j_s) \in \mathcal{T}_\delta^n \right\} \tag{26}$$

$$\mathcal{D}^n \triangleq \{d(s^n, z^n) : s^n \in \mathcal{S}^n, z^n \in \mathcal{Z}^n\} \tag{27}$$

$$\gamma_{\mathcal{C}_S}(j_p) \triangleq \sum_{j_s=1}^{2^{nR_K}} 1\{S^n(j_p, j_s) \in \mathcal{T}_\delta^n\} \tag{28}$$

$$\phi_{\mathcal{C}_S}(s^n) \triangleq \sum_{j \in [2^{nR}]} 1\{S^n(j) = s^n\} \tag{29}$$

Obviously the events $\mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4$ are only about $\mathcal{C}_S$, while the event $\mathcal{A}_1$ is about S^n and $\mathcal{C}_S$. The δ-typical set is defined according to the notion of strong typicality, see [11]:

$$\mathcal{T}_\delta^n(S) \triangleq \{s^n \in \mathcal{S}^n : |T_{s^n} - P_S| < \delta P_S\}, \tag{30}$$

where T_{s^n} denotes the empirical distribution of s^n (i.e., the type of s^n).

Next we will prove that any codebook $\mathcal{C}_S$ that makes the events $\mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4$ hold will also make the wiretapper decrypt the source with vanish probability. First, by method of types, we can prove the Lemmas 1-3.

Lemma 1. *For any $\epsilon > 0$ and small enough δ, $\mathbb{P}_{\mathcal{C}_S}\left[\overline{\mathcal{A}_2}\right] \to 0$, as $n \to \infty$.*

Lemma 2. *For any $\epsilon > 0$ and small enough δ, $\mathbb{P}_{\mathcal{C}_S}\left[\overline{\mathcal{A}_3}\right] \to 0$, as $n \to \infty$.*

Lemma 3. *For any $\epsilon > 0$ and small enough δ, $\mathbb{P}_{\mathcal{C}_S}\left[\overline{\mathcal{A}_4}\right] \to 0$, as $n \to \infty$.*

The proofs of Lemmas 1, 2 and 3 are given in Appendixes C, D and E, respectively.

In addition, denote

$$Q_i \triangleq \begin{cases} 1, & \text{if Node A encodes } i\text{th subblock successfully} \\ 0, & \text{otherwise} \end{cases} \tag{31}$$

Observe that Node A encodes ith subblock successfully, if and only if $\mathcal{A}_1$ happens; otherwise, randomly choose J. Therefore,

$$\mathbb{P}(Q_i | \mathcal{C}_S, \mathcal{A}) = \begin{cases} \mathbb{P}_{S^n}\left[\mathcal{A}_1 | \mathcal{C}_S, \mathcal{A}\right], & \text{if } Q_i = 1 \\ \mathbb{P}_{S^n}\left[\overline{\mathcal{A}_1} | \mathcal{C}_S, \mathcal{A}\right], & \text{otherwise} \end{cases} \tag{32}$$

where $\mathcal{A} \triangleq \mathcal{A}_2 \mathcal{A}_3 \mathcal{A}_4$.

Lemma 4. *For any $\delta > 0$, if $R \geq H(S) + \epsilon$, then $\mathbb{P}_{S^n}\left[\overline{\mathcal{A}_1} | \mathcal{C}_S, \mathcal{A}\right] \to 0$, as $n \to \infty$.*

The proof of Lemma 4 is given in Appendix F.

In the following, we denote $\epsilon_n \triangleq \mathbb{P}_{S^n}\left[\overline{\mathcal{A}_1} | \mathcal{C}_S, \mathcal{A}\right]$. Observe that Q^l is a sequence of i.i.d. random variables. Define

$$\mathcal{A}_5 \triangleq \left\{Q^l \in \mathcal{T}_\delta^l(Q)\right\}, \tag{33}$$

then by the property of typicality we have the following lemma.

Lemma 5. *For any $\delta > 0$, $\mathbb{P}_{Q^l}\left[\overline{\mathcal{A}_5} | \mathcal{C}_S, \mathcal{A}\right] \to 0$, as $l \to \infty$.*

We add Q^l to the side information at both henchman and wiretapper. Obviously, this will not decrease the decryption performance of henchman and wiretapper. Therefore, to prove Theorem 2, we only need to show

$$\lim_{n\to\infty} \mathbb{P}_{\mathcal{C}_S}\left[\limsup_{l\to\infty} \mathbb{E}_{M^l Q^l} \max_{Hcode \in \mathcal{H}_{l, R_H - \epsilon}} \mathbb{P}[d\left(S^{nl}, Z^{nl}\right) \leq D_E] > \tau_n \right] = 0$$

i.e.,

$$\lim_{n\to\infty} \mathbb{P}_{\mathcal{C}_S}\left[\limsup_{l\to\infty} \mathbb{E}_{M^l Q^l}\left[\max_{Hcode \in \mathcal{H}_{l, R_H - \epsilon}} \mathbb{P}\left[d\left(S^{nl}, Z^{nl}\right) \leq D_E | M^l Q^l \mathcal{C}_S\right] | \mathcal{C}_S \right] > \tau_n \right] = 0$$

where Hcodes denote the henchman codes with side information $M^l Q^l$ at both henchman and wiretapper.

First restrict the $\mathcal{C}_S$ to satisfy $\mathcal{A}$ by utilizing Lemmas 1-3.

$$\begin{aligned}
&\mathbb{P}_{\mathcal{C}_S}\Big[\limsup_{l\to\infty}\mathbb{E}_{M^lQ^l}\\
&\max_{Hcode\in\mathcal{H}_{l,R_H-\epsilon}}\mathbb{P}[d\left(S^{nl},Z^{nl}\right)\le D_E]>\tau_n\Big]\\
\le&\mathbb{P}_{\mathcal{C}_S}\Big[\limsup_{l\to\infty}\mathbb{E}_{M^lQ^l}\\
&\max_{Hcode\in\mathcal{H}_{l,R_H-\epsilon}}\mathbb{P}[d\left(S^{nl},Z^{nl}\right)\le D_E]>\tau_n|\mathcal{A}\Big]+\mathbb{P}_{\mathcal{C}_S}[\overline{\mathcal{A}}]\\
\le&\mathbb{P}_{\mathcal{C}_S}\Big[\limsup_{l\to\infty}\mathbb{E}_{M^lQ^l}\\
&\max_{Hcode\in\mathcal{H}_{l,R_H-\epsilon}}\mathbb{P}[d\left(S^{nl},Z^{nl}\right)\le D_E]>\tau_n|\mathcal{A}\Big]+\epsilon_n \quad (34)
\end{aligned}$$

where $\mathcal{H}_{l,R_H-\epsilon}\triangleq\{(l,R'_H)\,Hcode:\ R'_H\le R_H-\epsilon\}$.

We also restrict the Q^l to satisfy $\mathcal{A}_5$ by utilizing Lemma 5.

$$\begin{aligned}
&\limsup_{l\to\infty}\mathbb{E}_{M^lQ^l}\Big[\max_{Hcode\in\mathcal{H}_{l,R_H-\epsilon}}\\
&\mathbb{P}\left[d\left(S^{nl},Z^{nl}\right)\le D_E|M^lQ^l\mathcal{AC}_S\right]|\mathcal{AC}_S\Big]\\
\le&\limsup_{l\to\infty}\mathbb{E}_{M^lQ^l}\Big[\max_{Hcode\in\mathcal{H}_{l,R_H-\epsilon}}\\
&\mathbb{P}\left[d\left(S^{nl},Z^{nl}\right)\le D_E|M^lQ^l\mathcal{A}_5\mathcal{AC}_S\right]|\mathcal{A}_5\mathcal{AC}_S\Big]\\
&+\limsup_{l\to\infty}\mathbb{P}_{Q^l}\left[\overline{\mathcal{A}_5}|\mathcal{AC}_S\right]\\
=&\limsup_{l\to\infty}\mathbb{E}_{M^lQ^l}\Big[\max_{Hcode\in\mathcal{H}_{l,R_H-\epsilon}}\\
&\mathbb{P}\left[d\left(S^{nl},Z^{nl}\right)\le D_E|M^lQ^l\mathcal{A}_5\mathcal{AC}_S\right]|\mathcal{A}_5\mathcal{AC}_S\Big]
\end{aligned}$$

We can consider all possible sequences z^{nl} given $(\mathcal{C}_S,M^lQ^l)$ as a codebook. Since the wiretapper only receives R_H rate message from the henchman, possible sequences z^{nl} given $(\mathcal{C}_S,M^lQ^l)$ produced by it is not more than 2^{nlR_H}. Then a Hcode could be seen as the combination of a codebook (with size 2^{nlR_H}) of z^n sequences and an encoder that is designed based on that codebook. Hence we can write

$$\begin{aligned}
&\max_{Hcode\in\mathcal{H}_{l,R_H-\epsilon}}\mathbb{P}[d(S^{nl},Z^{nl})\le D_E|M^lQ^l\mathcal{A}_5\mathcal{AC}_S]\\
=&\max_{c_{\mathsf{z}}(\mathcal{C}_S,M^lQ^l)}\mathbb{P}\Big[\min_{z^{nl}\in c_{\mathsf{z}}(\mathcal{C}_S,M^lQ^l)}d(S^{nl},z^{nl})\le D_E|M^lQ^l\mathcal{A}_5\mathcal{AC}_S\Big], \quad (35)
\end{aligned}$$

where the notation $c_{\mathsf{z}}(\mathcal{C}_S,M^lQ^l)$ emphasizes that c_{z} is a function of the random codebook $\mathcal{C}_S$ and public messages $(\mathcal{C}_S,M^lQ^l)$. Then by using a union bound, we can write the right-hand side of (35) as

$$\begin{aligned}
&\mathbb{P}\Big[\min_{z^{nl}\in c_{\mathsf{z}}(\mathcal{C}_S,M^lQ^l)}d(S^{nl},z^{nl})\le D_E|M^lQ^l\mathcal{A}_5\mathcal{AC}_S\Big]\\
\overset{(a)}{\le}&\sum_{z^{nl}\in c_{\mathsf{z}}(\mathcal{C}_S,M^lQ^l)}\mathbb{P}\Big[d(S^{nl},z^{nl})\le D_E|M^lQ^l\mathcal{A}_5\mathcal{AC}_S\Big] \quad (36)\\
\le&2^{nlR_H}\max_{z^{nl}\in c_{\mathsf{z}}(\mathcal{C}_S,M^lQ^l)}\mathbb{P}\Big[d(S^{nl},z^{nl})\le D_E|M^lQ^l\mathcal{A}_5\mathcal{AC}_S\Big] \quad (37)\\
\le&2^{nlR_H}\max_{z^{nl}\in\mathcal{Z}^{nl}}\mathbb{P}\Big[d(S^{nl},z^{nl})\le D_E|M^lQ^l\mathcal{A}_5\mathcal{AC}_S\Big] \quad (38)\\
\overset{(b)}{\le}&2^{nlR_H}\max_{z^{nl}\in\mathcal{Z}^{nl}}\mathbb{P}\Big[\sum_{i=1}^{t}d(S_i^n(J_i),z_i^n)\le lD_E|M^lQ^l\mathcal{A}_5\mathcal{AC}_S\Big] \quad (39)\\
=&2^{nlR_H}\max_{z^{nl}\in\mathcal{Z}^{nl}}\mathbb{P}\Big[\sum_{i=1}^{t}d(S_i^n(J_i),z_i^n)\le lD_E|Q^t=1,M^t,\mathcal{A},\mathcal{C}_S\Big] \quad (40)\\
=&2^{nlR_H}\max_{z^{nt}\in\mathcal{Z}^{nt}}\sum_{j_1,\cdots,j_t}\prod_{i=1}^{t}\mathbb{P}\left[J_i=j_i|Q_i=1,M_i=m_i,\mathcal{A},\mathcal{C}_S\right]\\
&1\left\{\sum_{i=1}^{t}d(S_i^n(J_i),z_i^n)\le lD_E\right\} \quad (41)
\end{aligned}$$

where step (a) is a union bound, and step (b) follows from that 1) by definition of typicality, the number of "1" in Q^l is at least $l\,(1-\delta)\,(1-\epsilon_n)$, and $t\triangleq l\,(1-\delta)\,(1-\epsilon_n)$, 2) without loss of generalization we assume $Q_i=1,1\le i\le t$. Now we derive the probability $\mathbb{P}\left[J_i=j_i|Q_i=1,M_i=m_i\right]$. For different i, (J_i,M_i,Q_i) is i.i.d., hence for simplicity, we use $\mathbb{P}\left[J=j|Q=1,M=m\right]$ to denote $\mathbb{P}\left[J_i=j_i|Q_i=1,M_i=m_i\right]$. Moreover, for simplicity, we also omit condition $\mathcal{A},\mathcal{C}_S$ for each probability expression. First we have

$$\begin{aligned}
&\mathbb{P}\left[S^n=s^n,J=j,Q=1,M=m\right]\\
=&\mathbb{P}\left[S^n=s^n,J=j,M=m,S^n\in\mathcal{T}_\delta^n,S^n\in\mathcal{C}_S\right] \quad (42)\\
=&\mathbb{P}\left[S^n=s^n,S^n\in\mathcal{T}_\delta^n,S^n\in\mathcal{C}_S\right]\\
&\times\mathbb{P}\left[J=j|S^n=s^n,S^n\in\mathcal{T}_\delta^n,S^n\in\mathcal{C}_S\right]\mathbb{P}\left[M=m|J=j\right]. \quad (43)
\end{aligned}$$

For first term of 43, we have

$$\begin{aligned}
&\mathbb{P}\left[S^n=s^n,S^n\in\mathcal{T}_\delta^n,S^n\in\mathcal{C}_S\right]\\
=&\mathbb{P}\left[S^n=s^n\right]1\left\{s^n\in\mathcal{T}_\delta^n,s^n\in\mathcal{C}_S\right\} \quad (44)
\end{aligned}$$

and

$$2^{-n(H(S)+\epsilon)}\le\mathbb{P}\left[S^n=s^n\right]\le2^{-n(H(S)-\epsilon)},if\,s^n\in\mathcal{T}_\delta^n \quad (45)$$

where (45) is the property of typicality [11]. For other terms of 43, we have

$$\begin{aligned}
&\mathbb{P}\left[J=j|S^n=s^n,S^n\in\mathcal{T}_\delta^n,S^n\in\mathcal{C}_S\right]\\
\ge&2^{-n(R-H(S)+\epsilon)}1\left\{S^n(j)=s^n\right\} \quad (46)
\end{aligned}$$

$$\begin{aligned}&\mathbb{P}\left[J=j|S^n=s^n,S^n\in\mathcal{T}_\delta^n,S^n\in\mathcal{C}_S\right]\\ \le&2^{-n(R-H(S)-\epsilon)}1\left\{S^n\left(j\right)=s^n\right\}\end{aligned}\tag{47}$$

and

$$\mathbb{P}\left[M=m|J=j\right]=2^{-nR_K}1\left\{m_p=j_p\right\}\tag{48}$$

where (46) and (47) follow from the encoding process and the condition $\mathcal{C}_S$ satisfying $\mathcal{A}_4$.

Therefore,

$$\begin{aligned}&\mathbb{P}\left[J=j|M=m,Q=1\right]\\ =&\frac{\sum_{s^n\in\mathcal{S}^n}\mathbb{P}\left[S^n=s^n,J=j,Q=1,M=m\right]}{\sum_{j\in[2^{nR}]}\sum_{s^n\in\mathcal{S}^n}\mathbb{P}\left[S^n=s^n,J=j,Q=1,M=m\right]}\end{aligned}\tag{49}$$

$$\le\frac{\sum_{s^n\in\mathcal{S}^n}2^{-n(H(S)-\epsilon)}1\left\{s^n\in\mathcal{T}_\delta^n,s^n\in\mathcal{C}_S\right\}...}{\sum_{j\in[2^{nR}]}\sum_{s^n\in\mathcal{S}^n}2^{-n(H(S)+\epsilon)}1\left\{s^n\in\mathcal{T}_\delta^n,s^n\in\mathcal{C}_S\right\}...}$$

$$\frac{2^{-n(R-H(S)-\epsilon)}1\left\{S^n\left(j\right)=s^n\right\}2^{-nR_K}1\left\{m_p=j_p\right\}}{2^{-n(R-H(S)+\epsilon)}1\left\{S^n\left(j\right)=s^n\right\}2^{-nR_K}1\left\{m_p=j_p\right\}}\tag{50}$$

$$\le\frac{2^{n4\epsilon}1\left\{S^n\left(j\right)\in\mathcal{T}_\delta^n,S^n\left(j\right)\in\mathcal{C}_S\right\}1\left\{m_p=j_p\right\}}{\sum_{j\in[2^{nR}]}1\left\{S^n\left(j\right)\in\mathcal{T}_\delta^n,S^n\left(j\right)\in\mathcal{C}_S\right\}1\left\{m_p=j_p\right\}}\tag{51}$$

$$=\frac{2^{n4\epsilon}1\left\{S^n\left(j\right)\in\mathcal{T}_\delta^n\right\}1\left\{m_p=j_p\right\}}{\sum_{j\in[2^{nR}]}1\left\{S^n\left(j\right)\in\mathcal{T}_\delta^n\right\}1\left\{m_p=j_p\right\}}\tag{52}$$

$$\le\frac{2^{n4\epsilon}1\left\{S^n\left(j\right)\in\mathcal{T}_\delta^n\right\}1\left\{m_p=j_p\right\}}{\sum_{j_s\in\left[2^{nR_K}\right]}1\left\{S^n\left(m_p,j_s\right)\in\mathcal{T}_\delta^n\right\}}\tag{53}$$

$$\le\frac{2^{n4\epsilon}1\left\{S^n\left(j\right)\in\mathcal{T}_\delta^n\right\}1\left\{m_p=j_p\right\}}{\left(1-\epsilon\right)2^{nR_K}}\tag{54}$$

where (54) follows from the condition $\mathcal{C}_S$ satisfying $\mathcal{A}_3$.

Combining (41) and (54), we have

$$\begin{aligned}&\mathbb{P}\Big[\min_{z^{nl}\in c_z(\mathcal{C}_S,M^lQ^l)}d(S^{nl},z^{nl})\le D_E|M^lQ^l\mathcal{A}_5\mathcal{A}\mathcal{C}_S\Big]\\ \le&\mu\max_{z^{nt}\in\mathcal{Z}^{nt}}\sum_{j_{s,1},\cdots,j_{s,t}}\prod_{i=1}^t1\left\{S^n\left(m_{p,i},j_{s,i}\right)\in\mathcal{T}_\delta^n\right\}\\ &1\{\sum_{i=1}^t d(S^n(m_{p,i},j_{s,i}),z_i^n)\le lD_E\}\end{aligned}\tag{55}$$

$$\begin{aligned}\le&\mu\max_{z^{nt}\in\mathcal{Z}^{nt}}\sum_{j_{s,1}=1}^{2^{nR_K}}\sum_{j_{s,2}=1}^{2^{nR_K}}\cdots\sum_{j_{s,t}=1}^{2^{nR_K}}\sum_{D_1,D_2,\cdots,D_t:\sum_{i=1}^t D_i\le lD_E}\\ &\prod_{i=1}^t1\{d(S^n(m_{p,i},j_{s,i}),z_i^n)=D_i,S^n(m_{p,i},j_{s,i})\in\mathcal{T}_\delta^n\}\end{aligned}\tag{56}$$

$$\le\mu\sum_{D_1,D_2,\cdots,D_t:\sum_{i=1}^t D_i\le lD_E}\eta_1\eta_2\cdots\eta_t\tag{57}$$

$$\overset{(a)}{=}\mu2^{O(l\log n)}\max_{D_1,D_2,\cdots,D_t:\sum_{i=1}^t D_i\le lD_E}\eta_1\eta_2\cdots\eta_t\tag{58}$$

where $\mu=\frac{1}{(1-\epsilon)^t}2^{nlR_H-nt(R_K-4\epsilon)}$,

$$\eta_i\triangleq\max_{m_{p,i}\in\left[2^{n(R-R_K)}\right]}\max_{z_i^n\in\mathcal{Z}^n}\tag{59}$$

$$\sum_{j_{s,i}=1}^{2^{nR_K}}1\{d(S^n(m_{p,i},j_{s,i}),z_i^n)\le D_i,S^n(m_{p,i},j_{s,i})\in\mathcal{T}_\delta^n\}\tag{60}$$

and step (a) follows from that the number of the distortion incurred by n length block is at most polynomial in n, see Appendix A.

Combining (34), (35), and (58), we have (61) (at top of the next page), where $\mu_2=\tau_n\left(1-\epsilon\right)^t2^{nt(R_K-4\epsilon)-nlR_H-O(l\log n)}$.

Therefore, we only need to prove when $\mathcal{C}_S=c$ make $\mathcal{A}_2$ hold, then there exists a large enough n (not dependent on l) that makes the following hold for any l.

$$\max_{D_1,D_2,\cdots,D_t:\sum_{i=1}^t D_i\le lD_E}\eta_1\eta_2\cdots\eta_t\le\mu_2\tag{63}$$

Assume $\mathcal{A}_2$ holds, then we have

$$\begin{aligned}&\max_{D_1,D_2,\cdots,D_t:\sum_{i=1}^t D_i\le lD_E}\eta_1\eta_2\cdots\eta_t\\ \le&\max_{D_1,D_2,\cdots,D_t:\sum_{i=1}^t D_i\le lD_E}\prod_{i=1}^t2^{n\left([R_K-R(D_i)]^+\right.+\epsilon)}\end{aligned}\tag{64}$$

Hence we only need show

$$\max_{D_1,D_2,\cdots,D_t:\sum_{i=1}^t D_i\le lD_E}\prod_{i=1}^t2^{n\left([R_K-R(D_i)]^+\right.+\epsilon)}\le\mu_2\tag{65}$$

Assume there are b of D_i such that $R_K>R(D_i)$ in t subblocks, and $\lambda\triangleq\frac{b}{t}$. Then we have

$$\begin{aligned}&\max_{D_1,D_2,\cdots,D_t:\sum_{i=1}^t D_i\le lD_E}\prod_{i=1}^t2^{n\left([R_K-R(D_i)]^+\right.+\epsilon)}\\ \le&\max_{\lambda,D_1,D_2,\cdots,D_{\lambda t}:\sum_{i=1}^{\lambda t}D_i\le lD_E}2^{tn\epsilon}2^{\lambda tnR_K}2^{-n\sum_{i=1}^{\lambda t}R(D_i)}\end{aligned}\tag{66}$$

$$\le\max_{\lambda,D:\lambda tD\le lD_E}2^{tn\epsilon}2^{\lambda tn(R_K-R(D))}\tag{67}$$

$$=2^{tn\epsilon+\max_{\lambda,D:\lambda tD\le lD_E}[\lambda tn(R_K-R(D))]}\tag{68}$$

For sufficiently n, all subexponential terms in μ_2 can be omitted, hence we only need show

$$2^{tn\epsilon+\max_{\lambda,D:\lambda tD\le lD_E}[\lambda tn(R_K-R(D))]}\le2^{nt(R_K-4\epsilon)-nlR_H}$$

i.e.,

$$\begin{aligned}R_H\le&\frac{1}{l}\left[t\left(R_K-4\epsilon\right)-t\epsilon-\max_{\lambda,D:\lambda tD\le lD_E}\left[\lambda t\left(R_K-R(D)\right)\right]\right]\\ =&\frac{t}{l}\left[-5\epsilon+\min_{\lambda,D:\lambda D\le\frac{t}{l}D_E}\left[\left(1-\lambda\right)R_K+\lambda R(D)\right]\right]\end{aligned}\tag{69}$$

$$
\begin{aligned}
&\mathbb{P}_{\mathcal{C}_S}\Big[\limsup_{l\to\infty}\mathbb{E}_{M^lQ^l}\max_{Hcode\in\mathcal{H}_{l,R_H-\epsilon}}\mathbb{P}[d(S^{nl},Z^{nl})\le D_E]>\tau_n\Big]\\
&\le\mathbb{P}_{\mathcal{C}_S}\left[\limsup_{l\to\infty}\mathbb{E}_{M^lQ^l}\left[\max_{c_z(\mathcal{C}_S,M^lQ^l)}\mathbb{P}\Big[\min_{z^{nl}\in c_z(\mathcal{C}_S,M^lQ^l)}d(S^{nl},z^{nl})\le D_E|M^lQ^l\mathcal{A}_5\mathcal{A}\mathcal{C}_S\Big]|\mathcal{A}_5\mathcal{A}\mathcal{C}_S\right]>\tau_n|\mathcal{A}\right]+\epsilon_n\\
&\le\mathbb{P}_{\mathcal{C}_S}\left[\limsup_{l\to\infty}\mathbb{E}_{M^lQ^l}\left[\max_{D_1,D_2,\cdots,D_t:\sum_{i=1}^t D_i\le lD_E}\eta_1\eta_2\cdots\eta_t|\mathcal{A}_5\mathcal{A}\mathcal{C}_S\right]>\mu_2|\mathcal{A}\right]+\epsilon_n\\
&=\mathbb{P}_{\mathcal{C}_S}\left[\limsup_{l\to\infty}\max_{D_1,D_2,\cdots,D_t:\sum_{i=1}^t D_i\le lD_E}\eta_1\eta_2\cdots\eta_t>\mu_2|\mathcal{A}\right]+\epsilon_n
\end{aligned}\tag{61}
$$

For small enough δ, ϵ and large enough n, we have

$$\frac{t}{l}=(1-\delta)(1-\epsilon_n)\to 1$$

Then (69) becomes

$$R_H\le\min_{\lambda,D:\lambda D\le D_E}\left[(1-\lambda)R_K+\lambda R(D)\right]$$

This is just the condition of Theorem (2). Hence the achievability of Theorem 2 holds. ∎

Appendix C
Proof of Lemma 1

Proof: According to definition of $\mathcal{A}_2$,

$$\mathbb{P}_{\mathcal{C}_S}\left[\overline{\mathcal{A}_2}\right]\tag{70}$$

$$=\mathbb{P}_{\mathcal{C}_S}\left[\begin{array}{l}\max\limits_{j_p\in\left[2^{n(R-R_K)}\right]}\max\limits_{z^n\in Z^n}\eta_{\mathcal{C}_S,D}(z^n,j_p)\\ >2^{n\left([R_K-R(D)]^+\epsilon\right)},\exists D\in\mathcal{D}^n\end{array}\right]\tag{71}$$

$$\le|\mathcal{Z}^n|\,2^{n(R-R_K)+O(\log n)}\max_{j_p\in\left[2^{n(R-R_K)}\right]}\max_{D\in\mathcal{D}^n}\max_{z^n\in Z^n}\mathbb{P}_{\mathcal{C}_S}\left[\eta_{\mathcal{C}_S,D}(z^n,j_p)>2^{n\left([R_K-R(D)]^+\epsilon\right)}\right]\tag{72}$$

where (72) follows from a union bound and the fact $|\mathcal{D}^n|$ is polynomial in n, see Appendix A. Define $\xi_{j_p,j_s,z^n}\triangleq 1\left\{d(S^n(j_p,j_s),z^n)\le D,S^n(j_p,j_s)\in\mathcal{T}_\delta^n\right\}$, then $\eta_{z^n,\mathcal{C}_S(j_p)}=\sum_{j_s=1}^{2^{nR_K}}\xi_{j_p,j_s,z^n}$. Given j_p and z^n, $\xi_{j_p,j_s,z^n},j_s\in\left[2^{nR_K}\right]$ are i.i.d. random variables, with mean

$$\mathbb{E}_{\mathcal{C}_S}\xi_{j_p,j_s,z^n}=\mathbb{P}\left\{d(S^n,z^n)\le D_E,S^n\in\mathcal{T}_\delta^n\right\}\tag{73}$$

If we can show that the probability in (72) decays doubly exponentially fast with n, then the proof will be complete. To that end, we first introduce the following lemmas.

Lemma 6. *[6], [7] If S^n is i.i.d. according to P_S, then for any z^n,*

$$\mathbb{P}[d(S^n,z^n)\le D,S^n\in\mathcal{T}_\delta^n]\le 2^{-n(R(D)-o(1))},\tag{74}$$

where $R(D)$is the point-to-point rate-distortion function for P_S , and $o(1)$ is a term that vanishes as $\delta\to 0$ and $n\to\infty$.

Lemma 7. *[6], [7] If X^m is a sequence of i.i.d. Bern(p) random variables, then*

$$\mathbb{P}\Big[\sum_{i=1}^m X_i>k\Big]\le\left(\frac{emp}{k}\right)^k.\tag{75}$$

From Lemma 6, we see that

$$\mathbb{E}_{\mathcal{C}_S}\xi_{j_p,j_s,z^n}\le 2^{-n(R(D)-o(1))}\tag{76}$$

Using the bound on $\mathbb{E}[\xi_{j_p,j_s,z^n}]$, we can apply Lemma 7 to the probability in (72) by identifying

$$\begin{aligned}m&=2^{nR_K}\\ p&\le 2^{-n(R(D)-o(1))}\\ k&=2^{n\left([R_K-R(D)]^+\epsilon\right)}.\end{aligned}\tag{77}$$

This gives

$$\mathbb{P}\Big[\sum_{j=1}^{2^{nR_K}}\xi_{j_p,j_s,z^n}>2^{n\left([R_K-R(D)]^+\epsilon\right)}\Big]\le 2^{-n\alpha 2^{n\beta}},\tag{78}$$

where

$$\begin{aligned}\alpha&=[R_K-R(D)]^+-(R_K-R(D))+\epsilon-o(1)\\ \beta&=[R_K-R(D)]^++\epsilon.\end{aligned}\tag{79}$$

For any fixed ϵ and large enough n, both α and β are positive and bounded away from zero, and (78) vanishes doubly exponentially fast. Consequently, the expression in (72) vanishes, completing the proof of Lemma 1. ∎

Appendix D
Proof of Lemma 2

Proof: According to definition of $\mathcal{A}_3$,

$$\mathbb{P}_{\mathcal{C}_S}\left[\overline{\mathcal{A}_3}\right]\tag{80}$$

$$=\mathbb{P}_{\mathcal{C}_S}\left[\min_{j_p\in\left[2^{n(R-R_K)}\right]}\gamma_{\mathcal{C}_S(j_p)}<(1-\epsilon)2^{nR_K}\right]\tag{81}$$

$$\le 2^{n(R-R_K)}\max_{j_p\in\left[2^{n(R-R_K)}\right]}\mathbb{P}_{\mathcal{C}_S}\left[\gamma_{\mathcal{C}_S(j_p)}<(1-\epsilon)2^{nR_K}\right]\tag{82}$$

Define $\zeta_{j_p,j_s}\triangleq 1\{S^n(j_p,j_s)\in\mathcal{T}_\delta^n\}$, then $\gamma_{\mathcal{C}_S(j_p)}=\sum_{j_s=1}^{2^{nR_K}}\zeta_{j_p,j_s}$. Given j_p , $\zeta_{j_p,j_s},j_s\in\left[2^{nR_K}\right]$ are i.i.d. random variables, with mean

$$\mathbb{E}_{\mathcal{C}_S}\zeta_{j_p,j_s} \tag{83}$$
$$= \mathbb{P}\left\{S^n(j) \in \mathcal{T}_\delta^n\right\} \tag{84}$$
$$\geq 1-\epsilon_2 \tag{85}$$

where (85) holds for any $\epsilon_2 > 0$ and sufficiently large n, and it follows from the typicality property. If we can show that the probability in (82) decays doubly exponentially fast with n, then the proof will be complete. To that end, we first introduce the following lemma on Chernoff bound.

Lemma 8. *[12] If X^m is a sequence of i.i.d. Bern(p) random variables, then*

$$\mathbb{P}\Big[\sum_{i=1}^{m} X_i \leq (1-\delta)mp\Big] \leq e^{-\frac{\delta^2 mp}{2}}, 0 \leq \delta \leq 1. \tag{86}$$

By indentifying that

$$m = 2^{nR_K} \tag{87}$$
$$p \geq 1-\epsilon_2 \tag{88}$$
$$\delta \geq 1 - \frac{1-\epsilon}{1-\epsilon_2} \tag{89}$$

and applying Lemma 8, we have

$$\mathbb{P}_{\mathcal{C}_S}\left\{\gamma_{\mathcal{C}_S(j_p)} < (1-\epsilon)\,2^{nR_K}\right\} \leq e^{-\frac{\delta^2 mp}{2}} \leq e^{-\frac{\delta^2 m(1-\epsilon_2)}{2}} \tag{90}$$

For fixed ϵ, if δ is small enough and n is large enough, then $\epsilon_2 < \epsilon$ and $\epsilon_2 < 1$, which means that $\delta > 0$ and $1-\epsilon_2 > 0$. Hence (90) vanishes doubly exponentially fast. This completes the proof of Lemma 2. ∎

Appendix E
Proof of Lemma 3

Proof: According to definition of $\mathcal{A}_4$,

$$\mathbb{P}_{\mathcal{C}_S}\left[\mathcal{A}_4\right] \tag{91}$$
$$= \mathbb{P}_{\mathcal{C}_S}\left[\begin{array}{l}\max\limits_{s^n\in\mathcal{T}_\delta^n} \phi_{\mathcal{C}_S}(s^n) > 2^{n(R-H(S)+\epsilon)}, \\ or\ \min\limits_{s^n\in\mathcal{T}_\delta^n} \phi_{\mathcal{C}_S}(s^n) < 2^{n(R-H(S)-\epsilon)}\end{array}\right] \tag{92}$$
$$\leq \mathbb{P}_{\mathcal{C}_S}\left[\max_{s^n\in\mathcal{T}_\delta^n} \phi_{\mathcal{C}_S}(s^n) > 2^{n(R-H(S)+\epsilon)}\right] + \mathbb{P}_{\mathcal{C}_S}\left[\min_{s^n\in\mathcal{T}_\delta^n} \phi_{\mathcal{C}_S}(s^n) < 2^{n(R-H(S)-\epsilon)}\right] \tag{93}$$

In the following, we prove that both terms of (93) vanish as $n \to \infty$.

$$\mathbb{P}_{\mathcal{C}_S}\left[\max_{s^n\in\mathcal{T}_\delta^n} \phi_{\mathcal{C}_S}(s^n) > 2^{n(R-H(S)+\epsilon)}\right] \leq |\mathcal{T}_\delta^n| \max_{s^n\in\mathcal{T}_\delta^n} \mathbb{P}_{\mathcal{C}_S}\left[\phi_{\mathcal{C}_S}(s^n) > 2^{n(R-H(S)+\epsilon)}\right] \tag{94}$$

Define $\zeta_{j,s^n} \triangleq 1\{S^n(j) = s^n\}$, then $\phi_{\mathcal{C}_S}(s^n) = \sum_{j\in[2^{nR}]} \zeta_{j,s^n}$. Given $s^n \in \mathcal{T}_\delta^n$, $\zeta_{j,s^n}, j \in \left[2^{nR}\right]$ are i.i.d. random variables, with mean

$$\mathbb{E}_{\mathcal{C}_S}\zeta_{j,s^n} \tag{95}$$
$$= \mathbb{P}\left\{S^n(j) = s^n\right\} \tag{96}$$
$$\leq 2^{-n(H(S)-\epsilon_2(\delta))} \tag{97}$$

where $\epsilon_2(\delta)$ tends to zero as $\delta \to 0$, and (97) follows from the typicality property [11]. If we can show that the probability in (94) decays doubly exponentially fast with n, then the proof will be complete.

By indentifying that

$$m = 2^{nR} \tag{98}$$
$$p \leq 2^{-n(H(S)-\epsilon_2(\delta))} \tag{99}$$
$$k = 2^{n(R-H(S)+\epsilon)} \tag{100}$$

and applying Lemma 7, we have

$$\mathbb{P}_{\mathcal{C}_S}\left[\phi_{\mathcal{C}_S}(s^n) > 2^{n(R-H(S)+\epsilon)}\right] \leq 2^{-n\alpha 2^{n\beta}}, \tag{101}$$

where

$$\begin{aligned}\alpha &= \epsilon - \epsilon_2(\delta) \\ \beta &= R - H(S) + \epsilon.\end{aligned} \tag{102}$$

For fixed ϵ, if n is large enough and δ is small enough, then $\epsilon_2(\delta) < \epsilon$, which means that $\alpha > 0$ and $\beta > 0$. Hence (101) vanishes doubly exponentially fast. This means that (94) holds.

In the same way, by utilizing Lemma 8, we can prove that for small enough δ, as $n \to \infty$,

$$\mathbb{P}_{\mathcal{C}_S}\left[\min_{s^n\in\mathcal{T}_\delta^n} \phi_{\mathcal{C}_S}(s^n) < 2^{n(R-H(S)-\epsilon)}\right] \to 0 \tag{103}$$

Therefore, this completes the proof of Lemma 3. ∎

Appendix F
Proof of Lemma 4

Proof: According to definition of $\mathcal{A}_1$, we have

$$\mathbb{P}_{S^n}\left[\mathcal{A}_1|\mathcal{C}_S, \mathcal{A}\right] \tag{104}$$
$$= \mathbb{P}_{S^n}\left[S^n \in \mathcal{T}_\delta^n, S^n \in \mathcal{C}_S|\mathcal{C}_S, \mathcal{A}\right] \tag{105}$$
$$= \mathbb{P}_{S^n}\left[S^n \in \mathcal{T}_\delta^n|\mathcal{C}_S, \mathcal{A}\right]\mathbb{P}_{S^n}\left[S^n \in \mathcal{C}_S|S^n \in \mathcal{T}_\delta^n, \mathcal{C}_S, \mathcal{A}\right] \tag{106}$$
$$= \mathbb{P}_{S^n}\left[S^n \in \mathcal{T}_\delta^n|\mathcal{C}_S, \mathcal{A}\right] \tag{107}$$
$$= \mathbb{P}_{S^n}\left[S^n \in \mathcal{T}_\delta^n\right] \tag{108}$$

where (108) follows from that if $R \geq H(S)+\epsilon$, $S^n \in \mathcal{T}_\delta^n$ and $\mathcal{C}_S$ satisfying $\mathcal{A}_4$, then $S^n \in \mathcal{C}_S$. In addition, by law of large numbers, we have $\mathbb{P}_{S^n}\left[S^n \in \mathcal{T}_\delta^n\right] \to 1$ as $n \to \infty$ [11]. ∎